JOURNAL OF COMPUTER AND SYSTEM SCIENCES 49, 168–174 (1994)

Invariant Sets for Substitution

TAISHIN NISHIDA*

Faculty of Liberal Arts, Chukyo University, Showa-ku, Nagoya 466, Japan

AND

YOUICHI KOBUCHI†

Department of Biophysics, Faculty of Science, Kyoto University, Sakyo-ku, Kyoto 606, Japan

Received March 20, 1989; revised April 12, 1993

A relation F on a set X defines a function on the power set of X. A subset of X is said to be invariant for F if it is a fixed point for F. An element x of X is called ascendable in X if there exists an infinite sequence $x_0 = x, x_1, \ldots$, (not necessarily distinct) in X such that $x_i \in F(x_{i+1})$ $(i \geqslant 0)$. Then any invariant set Z is characterized as $Z = F^+(K)$ for some set K of ascendable elements, where F^+ stands for $\bigcup_{k=1} F^k$. In this note we prove that if F is a substitution over a finite alphabet, then for any invariant set Z there exists a set S of repeatable words such that $Z = F^+(S)$, in which a repeatable word u satisfies $u \in F^+(u)$.

INTRODUCTION

Let F be a binary relation on a countable set X. Then F determines a function from 2^X to 2^X (again denoted by F) as follows:

$$\text{For } Z \in 2^X, \qquad F(Z) = \{y \in X \mid \exists x \in Z, xFy\}.$$

We can thus define an n-fold product F^n of F for a nonnegative integer n as follows:

$$F^0 \text{ is the identity function on } 2^X, \qquad \text{and} \qquad F^{n+1} = F(F^n).$$

We shall use the following notations

$$F^* = \bigcup_{k \in \mathbf{N}} F^k, \qquad F^+ = F(F^*), \qquad \text{and} \qquad F^{[n]} = \bigcup_{k \in [n]} F^k,$$

* Present address: Faculty of Engineering, Toyama Prefectural University, Kosugi-Machi, Toyama 939-03, Japan, Email: nishida@pu-toyama.ac.jp

† Present address: Department of Electronics and Informatics, Ryukoku University, Seta, Otsu 520-21, Japan, Email: kobuchi@rins.ryukoku.ac.jp

0022-0000/94 $6.00

where $\mathbf{N}$ denotes the set of nonnegative integers and $[n]$ the set $\{0, 1, ..., n-1\}$ for any positive integer n. We shall not distinguish a singleton set $\{x\}$ from an element x. Also, we refer to a point Z in 2^X as a subset $Z \subseteq X$ whenever it is appropriate.

A subset $Z \subseteq X$ is called *invariant* for F if it is a fixed point with respect to F, i.e., $F(Z) = Z$.

We introduce ascendability concepts with respect to the function F as follows. Let Z be a subset of X. An element $x \in Z$ is said to be *ascendable in* Z if there exists an infinite sequence $x_0, x_1, ..., x_n, ...$ (not necessarily distinct) in Z such that $x = x_0$ and $x_i \in F(x_{i+1})$ $(i \geqslant 0)$. Also, $x \in X$ is called an *ascendable point* if it is ascendable in X. A subset Z is called *ascendable* if every $x \in Z$ is ascendable in Z. Then it is shown that an invariant set Z is the F^+ image of some ascendable subset K, i.e., $Z = F^+(K)$ (Lemma 1.3).

In addition to the above general characterization we can describe the structure of invariant sets in more detail in case F is defined by a substitution on a finite alphabet. Consider an element $x \in X$, called a *repeatable point*, such that $x \in F^+(x)$. It is obvious that for any repeatable point x, the set $F^+(x)$ is ascendable and $F^+(F^+(x)) = F^+(x)$ because $F^+(x) \subseteq F^+(F^+(x)) \subseteq F^+(x)$. Hence $F^+(x)$ is invariant. Then for any set S of repeatable points, the set $F^+(S)$ is also invariant. The converse is, however, not always the case. That is, in general, there is an ascendable point x such that there is no repeatable point z satisfying $x \in F^+(z)$.

The main result of this note is that if X is a free monoid over a finite set (or the set of all words over an alphabet) and F is a substitution on it, then for any ascendable point $x \in X$ there does exist a repeatable point z such that $x \in F^+(z)$ (Lemma 4.1). We also prove that any invariant set Z for a substitution is characterized as $Z = F^+(S)$ where S is a set of repeatable points (Theorem 4.3).

1. Invariant Set for a Multivalued Mapping

In this section, we prove several properties of invariant sets and ascendable sets.

Lemma 1.1. *A subset Z of X is ascendable if and only if $Z \subseteq F(Z)$.*

Proof. If part: If $Z \subseteq F(Z)$ then for every $x \in Z$ there exists some $y \in Z$ such that $x \in F(y)$. This guarantees that x is ascendable in Z.

Only if part: Let $x \in Z$. Since x is ascendable in Z, there is $y \in Z$ such that $x \in F(y)$. Thus $x \in F(Z)$. ∎

Property 1.2. (1) *$F(Z) = Z$ if and only if $F^+(Z) = Z$.*

(2) *If Z is invariant, then it is ascendable. Evidently, the converse is not necessarily true.*

(3) *If Z_1 and Z_2 are invariant (ascendable), then so is $Z_1 \cup Z_2$.*

The following lemma shows the relation beween invariant sets and ascendable sets.

LEMMA 1.3. *A subset Z of X is invariant if and only if $Z=F^+(K)$ for some ascendable subset K of X.*

Proof. Only if part: Since $Z=F(Z)=F^+(Z)$ and Z is ascendable, let $K=Z$.

If part: Since K is ascendable, we have $K\subseteq F(K)$ by Lemma 1.1. This implies $K\subseteq F^+(K)$ and $F^+(K)=K\cup F^+(K)$. Then, $F(Z)=F(F^+(K))=F(K\cup F^+(K))=F^+(K)=Z$. ∎

2. SUBSTITUTION OVER A FINITE ALPHABET

As we stated in Introduction, our main concern is the invariant sets for a substitution over a finite alphabet. In this section we give some necessary definitions and notations.

Let Σ be a finite set, which is called an *alphabet*. An element of Σ is called a *letter*. The set of all words over Σ, including the empty word 1, is denoted by Σ^*.

A subsequence of a word s is called a sparse subword of s or, for short, a *subword* of s. The *length* of a word s is denoted by $|s|$. If V is any subset of Σ, $|s|_V$ denotes the number of occurrences of letters of V in s.

DEFINITION. A relation F on Σ^* is said to be a substitution if it satisfies the following conditions.

(i) $F(1)=1$,

(ii) $F(a)\subseteq\Sigma^*$ for every $a\in\Sigma$, and

(iii) $F(w)=F(a_1)F(a_2)\cdots F(a_n)$ for every $w=a_1a_2\cdots a_n$ where $a_i\in\Sigma$ for $i=1, 2, ..., n$.

Let F be a substitution on Σ^*, and let u and v be two words in Σ^* such that $|u|=l$. The word v is said to be a *descendant* of u if v belongs to $F^n(u)$ for some positive integer n. The *derivation* Δ from u to v is an l-tuple of pairs $\Delta=((x_1, s_1), (x_2, s_2), ..., (x_l, s_l))$ where $u=x_1x_2\cdots x_l$, $v=s_1s_2\cdots s_l$, and $s_i\in F^n(x_i)$ for $i=1, 2, ..., l$.

A substitution F on Σ^* is said to be finite (resp. *rational, context free*) if $F(a)$ is a finite, (resp. rational, context free) subset of Σ^* for every a in Σ.

We assume the reader to be familiar with the basic notations and results of rational and context free languages (see, for example, [1]).

3. SOME TECHNICAL RESULTS

In this section we stablish some technical results, which will be useful in Section 4. Henceforth F will always denote a substitution on Σ^*, where Σ is a finite alphabet.

Repeatable points for a substitution are called repeatable words. We denote by $P(F)$ the set of repeatable words for F. i.e., $P(F)=\{w \mid w \in F^+(w)\}$. We note that a repeatable word u has at least one derivation Δ from u to u. Let $u=x_1 x_2 \cdots x_l$ $(x_i \in \Sigma,\ i=1,2,\ldots,l)$ and $\Delta=((x_1, s_1),(x_2, s_2),\ldots,(x_l, s_l))$ be a repeatable word and its derivation. Then u is said to be decomposed into $s_1 s_2 \cdots s_l$.

Many properties of the repeatable words have been studied in [2].

A letter a of Σ is said to be *vital* if 1 is not the descendant of a, i.e., $1 \notin F^+(a)$. The set of vital letters is denoted by V. The set of *nonvital* letters is denoted by N, i.e., $N=\Sigma-V=\{a \mid 1 \in F^+(a)\}$. A letter a of Σ is said to be *cyclic* if $uav \in F^+(a)$ for some $uv \in N^*$. We denote by C the set of cyclic letters.

LEMMA 3.1. *There is a positive integer n dependant only on F such that for any word $u=a_1 \cdots a_l$ in C^* there exists a repeatable word w in $F^n(u)$ where $w=s_0 a_1 s_1 \cdots s_{l-1} a_l s_l$ for some $s_0 \cdots s_l \in N^*$.*

Proof. For any cyclic letter a, there exists a positive integer k_a such that $uav \in F^{k_a}(a)$ for some $uv \in N^*$. Let K be the least common multiple of k_a for any $a \in C$. Let M be the minimum integer such that $1 \in F^M(b)$ for any $b \in N$. Let n be the least multiple of K that is larger than M, then $w=s_0 a_1 s_1 \cdots s_{l-1} a_l s_l$ is in $F^n(a_1 \cdots a_l)$ for some $s_0 \cdots s_l \in N^*$ and w is repeatable. ∎

Let $w \neq 1$ be ascendable and let $\sigma=(w_0, w_1, \ldots, w_n, \ldots)$ be an ascending sequence of w, where $w_0=w$. A *derivation trunk* of σ is a sequence of subwords u_i of w_i $(i=0, 1, \ldots)$ which is defined inductively by

(i) $u_0=w_0$.

(ii) Let $\Delta=((a_1, s_1),\ldots,(a_l, s_l))$ be a derivation from w_n to w_{n-1}, i.e., $w_n=a_1 \cdots a_l$ $(a_i \in \Sigma)$ and $w_{n-1}=s_1 \cdots s_l$ $(s_i \in \Sigma^*)$. Assume that $u_{n-1}=b_1 \cdots b_k$ is (inductively) given. Then we have $w_{n-1}=t_0 b_1 t_1 \cdots t_{k-1} b_k t_k$ for some $t_0 \cdots t_k \in \Sigma^*$. Let $s_{d_1}, \ldots, s_{d_m}$ $(1 \leqslant d_1 \leqslant d_2 < \cdots < d_m \leqslant l)$ be the subwords of w_{n-1} which contain at least one b_i's, i.e., for some $j \geqslant 1$, $s_{d_i}=t'_{f_i} b_{f_i+1} t_{f_i+1} \cdots b_{f_i+j} t'_{f_i+j}$ where t'_{f_i} is a suffix of t_{f_i} and t'_{f_i+j} is a prefix of t_{f_i+j} (see Fig. 1). Then u_n is defined as $u_n=a_{d_1} \cdots a_{d_m}$.

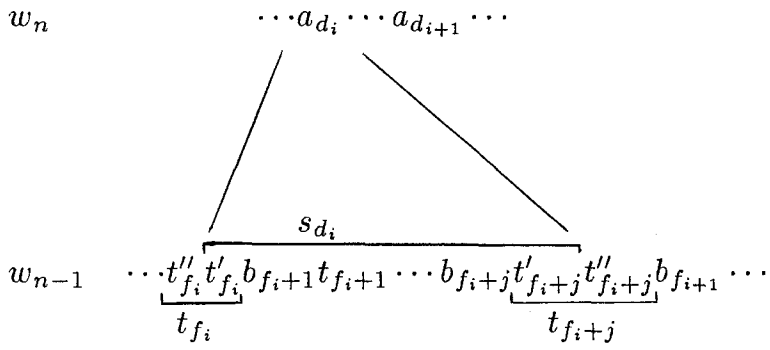

FIG. 1. Derivation from w_n to w_{n-1}, where $f_{i+1}=f_i+j+1$.

In the remainder of this section, let $w \neq 1$ be an ascending word, $\sigma = (w_0, w_1, ...)$ be an ascending sequence of w, and $(u_0, u_1, ...)$ be a derivation trunk of σ. Then we have the following properties and lemmas.

PROPERTY 3.2. (i) $|u_{n-1}| \geqslant |u_n|$ *and* $|u_n| > 0$ *for any* $n > 0$.

(ii) *There exists a positive integer* M *such that* $|u_M| = |u_{M+i}|$ *for any non-negative integer* i.

LEMMA 3.3. *For every* $n \geqslant 1$ *if* $u_n = a_1 \cdots a_k$ $(a_i \in \Sigma)$ *and* $w_n = t_0 a_1 t_1 \cdots t_{k-1} a_k t_k$ *for some* $t_0 \cdots t_k \in \Sigma^*$, *then* $1 \in F^n(t_0 \cdots t_k)$.

Proof. We prove this lemma by induction on n. For $n = 1$ the result directly follows from the definition. Suppose that $u_{n-1} = b_1 \cdots b_k$ and $w_{n-1} = t_0 b_1 t_1 \cdots t_{k-1} b_k t_k$ such that $1 \in F^{n-1}(t_0 \cdots t_k)$. Let $w_n = a_1 a_2 \cdots a_i$ $(a_i \in \Sigma)$, $u_n = a_{d_1} \cdots a_{d_m}$, and $\Delta = ((a_1, s_1), ..., (a_l, s_l))$ be the derivation process from w_n to w_{n-1}. Then, by the definition of the derivation trunk, every occurrence of b_i is contained in some s_{d_j}. On the other hand, every s_i for $i \notin \{d_1, ..., d_m\}$ is a subword of some t_j and $1 \in F^{n-1}(s_i) \subseteq F^n(a_i)$ because $1 \in F^{n-1}(t_j)$. Thus we have $w_n = v_0 a_{d_1} v_1 \cdots v_{m-1} a_{d_m} v_m$ such that $1 \in F^n(v_0 \cdots v_m)$. ∎

The proof of this lemma also shows the next corollary.

COROLLARY 3.4. (i) *If* $u_n = a_1 \cdots a_k$, *then* $w_n = t_0 a_1 t_1 \cdots t_{k-1} a_k t_k$ *for some* $t_0 \cdots t_k \in N^*$.

(ii) w_0 *is in* $F^n(u_n)$ *for any* $n \geqslant 0$.

LEMMA 3.5. *If* $u_n = u_{n'}$ *for some* $n \neq n'$, *then* u_n *is in* C^+.

Proof. Assume that $n > n'$. Let $u_n = a_1 \cdots a_j$. Then $w_{n'}$ is decomposed into $s_1 a_1 t_1 \cdots s_l a_l t_l$ such that $s'_l a_l t'_l \in F^{n-n'}(a_i)$ where s'_i is a suffix of s_i and t'_i is a prefix of t_i for $i = 1, ..., l$. Hence a_i is cyclic because $s'_i t'_i$ is in N^* for $i = 1, ..., l$ from Corollary 3.4(i). ∎

4. MAIN THEOREMS

In this section, we first establish the following lemmas, which state close relations beween ascendable words and repeatable words.

LEMMA 4.1. *If a word* x *is ascendable for a substitution* F, *then there exists a repeatable word* v *such that* $x \in F^+(v)$.

Proof. If $x = 1$, then x is in $F^+(1)$ and 1 is repeatable for any F. Then, assume that $x \neq 1$. Let $\sigma = (x_0, x_1, ...)$ be an ascending sequence of x and $(u_0, u_1, ...)$ be a corresponding derivation trunk of σ. By Property 3.2(ii), there is a pair u_n and $u_{n'}$ $(n \neq n')$ in the derivation trunk such that $u_n = u_{n'}$. Then $u_n = b_1 \cdots b_l$ is in C^+ from

Lemma 3.5. Let $v = s_o b_1 s_1 \cdots s_{l-1} b_l s_l$ be the repeatable word in $F^+(u_n)$ whose existence was proved in Lemma 3.1. By Corollary 3.4(ii), x is in $F^n(b_1 \cdots b_l)$. And we can assume that n is greater than the least integer M such that $1 \in F^M(s_0 \cdots s_l)$. Therefore we have $x \in F^+(v)$. ∎

LEMMA 4.2. *If a subset X of Σ^* is ascendable for a substitution F, then there exists a subset W of $P(F)$ such that $F^+(X) = F^+(W)$.*

Proof. For an ascendable word x, let $p(x)$ be the repeatable word whose existence is ensured by Lemma 4.1, i.e., $v = p(x) \in P(F)$ and $x \in F^+(v)$. Let $W = \{p(x) \mid x \in X\}$. Then we will show that $F^+(X) = F^+(W)$.

First we show that $F^+(X) \subseteq F^+(W)$. Let u be a word in $F^+(x)$ for some x in X. Then u is in $F^+(W)$ since $x \in F^+(p(x)) \subseteq F^+(W)$.

Next we show that $F^+(X) \supseteq F^+(W)$. Let u be a word in $F^+(v)$ for some v in W. By the definition of W, there is a word x in X such that $v = p(x)$. That is, there is a word u_n in the derivation trunk of the ascending sequence $\sigma = (x_0, x_1, \ldots)$ of x such that $v \in F^+(u_n)$ from the proof of the above lemma. Let x_n be the word in σ which corresponds to u_n. Since the letters contained in x_n which do not occur in u_n are nonvital and since v is repeatable, we have $v \in F^+(x_n)$. Because X is ascendable, we have $x_n \in X$ and hence the lemma follows immediately. ∎

Then we prove the main theorem.

THEOREM 4.3. *A subset X of Σ^* is invariant for F if and only if $X = F^+(S)$ for some $S \subseteq P(F)$.*

Proof. If part: For any subset S of $P(F)$, $F^+(S)$ is obviously ascendable. Then $F^+(F^+(S)) = F^+(S) = X$ is invariant by Lemma 1.3.

Only if part: If X is an invariant set, then there is an ascendable set Y such that $X = F^+(Y)$. By Lemma 4.2, there exists $W \subseteq P(F)$ such that $F^+(Y) = F^+(W) = X$. ∎

A subset $Z \subseteq X$ is said to be *maximum invariant* for F if Z is invariant and there is no invariant subset $Z' \subseteq X$ such that $Z \subset Z'$. We denote the maximum invariant set for F by $I(F)$.

COROLLARY 4.4. *The maximum invariant set for a substitution F is the image of the set of all repeatable words by the substitution, i.e.,*

$$I(F) = F^+(P(F)).$$

5. CONCLUDING REMARKS

Lemma 1.3 may be regarded as a special case of the following more general fixed point theorem.

THEOREM. *Let P be a partially ordered set and $\psi: P \to P$ be continous. Then $f \in P$ is a fixed point of ψ if and only if $f = \psi^+(h)$ $(= \bigcup_{k \geq 1} \psi^k(h))$ for some $h \in P$ such that $h \leqslant \psi(h)$.*

Similar results are also found, for example, in [3] and [4].

We have shown here that in the case of a mapping F defined by a substitution, any invariant set can be represented as $F^+(S)$ where S is a set of repeatable points, i.e., x's such that $x \in F^+(x)$. Note, however, that this is not the case for an arbitrary mapping F as shown below. Let $F: 2^N \to 2^N$ such that

$$F(n) = \begin{cases} n-2 & \text{if } n > 1 \\ n & \text{otherwise.} \end{cases}$$

Then there are only two repeatable points 0 and 1, but an invariant set $E = \{2i \mid i \in N\}$, for example, cannot be derived from 0 and/or 1.

REFERENCES

1. J. E. HOPCROFT AND J. D. ULLMAN, "Introduction to Automata Theory, Languages, and Computation," Addison–Wesley, Menlo Park, 1979.
2. T. NISHIDA AND Y. KOBUSHI, Repeatable words for substitution, *Theoret. Comput. Sci.* **53** (1987), 319–333.
3. E. SMITHSON, Fixed points of order preserving multifunctions, *Pro. Amer. Math.* **28** (1971), 304–310.
4. A. TARSKI, A lattice-theoretical fixpoint theorem and its applications, *Pacific J. Math.* **5** (1955), 285–309.